Written evidence submitted by Digital Net Identity UK Ltd. (OSB0143)

Objectives

1. Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

Digital Identity Net (DIN) believe that the Bill's approach to introduce accountability for content on user-to-user platforms via legislation, combined with technical solutions for improving the online environment, is a good approach and will achieve the policy aim to make the UK the safest place to be online. Digital identity solutions enable users to easily prove who they are online, and can be used to set up new accounts or verify existing accounts. These solutions can support 'real name displayed' and pseudonymous accounts (where the platform has traceability to the verified real user in cases of illegal content).

2. Will the proposed legislation help to deliver the policy aim of using digital technologies and services to support the UK's economic growth? Will it support a more inclusive, competitive, and innovative future digital economy?

The same technologies that can help with online safety will also help to support the UK's economic growth, and better enable an inclusive society via mechanisms such as increased access to Government data sets for those who are under-served today. The UK can build on its global reputation for building open, standards-based frameworks such as Open Banking, to deliver a world-leading approach to online safety based on the platforms verifying that their users are real people who have not been banned. This will enable the platform providers to provide a better product for their users; an environment without abusive comments or trolls, that also protects children from exposure to harmful content.

3. Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?

Yes, children can be protected if platform providers verify the ages of their users. This could be done to prove the users are over 18, for instance, and unsuitable content not shown unless the account has been verified.

4. Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?

5. Is the "duty of care" approach in the draft Bill effective?

6. Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

DIN agrees that the focus should be on systems and processes, and also include the ability for platforms to confirm answers to the questions 'who is the user who is posting the content?', 'who is the user consuming the content?' and 'are they over 18?'. AI technologies to filter content are constantly improving, but will never be able to 100% remove the risk that inappropriate content will be shown. Having a verifiable age would provide an absolute control over serving content to a user. Knowing the real identity of the posting account will also help with removing offenders, preventing them from creating new accounts, and enable fast reporting to law enforcement agencies for prosecution in the most serious cases.

7. How does the draft Bill differ to online safety legislation in other countries (e.g. Australia, Canada, Germany, Ireland, and the EU Digital Services Act) and what lessons can be learnt?

8. Does the proposed legislation represent a threat to freedom of expression, or are the protections for freedom of expression provided in the draft Bill sufficient?

Freedom of expression is still enabled under the framework of the Bill. Having a verified account still allows for the poster to express themselves. The account can also be pseudonymous to allow for a 'persona' to present someone's views without publicly declaring who they are. The 'persona' should be traceable by the platform back to a real person to dissuade posting of harmful or illegal content. Freedom of expression/ freedom of speech is not the same as 'free to say anything'.

Content in Scope

9. The draft Bill specifically includes CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

10. The draft Bill specifically places a duty on providers to protect democratic content, and content of journalistic importance. What is your view of these measures and their likely effectiveness?

11. Earlier proposals included content such as misinformation/disinformation that could lead to societal harm in scope of the Bill. These types of content have since been removed. What do you think of this decision?

12. Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

DIN would like to see specific reference to known fraud types that originate on user-to-user services, e.g. impersonation fraud where an account pretends to be a vendor, and obtains data or payment from an unsuspecting user victim, or romance scams. UK Finance collates industry information on fraud types and volumes for the UK FS industry; it would be good to see collaboration between public and private sector to define initial fraud types that could be included in the Bill, targeted and measured to see if the Bill approach is effective, and then apply this approach to other fraud types over time.

13. What would be a suitable threshold for significant physical or psychological harm, and what would be a suitable way for service providers to determine whether this threshold had been met?

14. Are the definitions in the draft Bill suitable for service providers to accurately identify and reduce the presence of legal but harmful content, whilst preserving the presence of legitimate content?

Services in Scope

15. The draft Bill applies to providers of user-to-user services and search services. Will this achieve the Government's policy aims? Should other types of services be included in the scope of the Bill?

16. The draft Bill sets a threshold for services to be designated as 'Category 1' services. What threshold would be suitable for this?

17. Are the distinctions between categories of services appropriate, and do they reliably reflect their ability to cause harm?

18. Will the regulatory approach in the Bill affect competition between different sizes and types of services?

Algorithms and user agency

19. What role do algorithms currently play in influencing the presence of certain types of content online and how it is disseminated? What role might they play in reducing the presence of illegal and/or harmful content?

AI technologies can be used to identify illegal or harmful content, but the identity behind the account is also needed to hold the user who owns the account responsible (otherwise illegal content can be posted by anonymous accounts with no accountability). AI content identification and digital identity technologies combined would give the best approach; to find the illegal content being posted, and to know who is doing it. There is little point in finding content and closing an account if the offender can just create a new account and re-post the material without any consequences. Certified digital identity technologies should be included in the 'Use of technology' approach to enable accountability. The certification can be provided by DCMS' Digital Identity Trust Framework, to join up different Government initiatives.

20. Are there any foreseeable problems that could arise if service providers increased their use of algorithms to fulfil their safety duties? How might the draft Bill address them?

21. Does the draft Bill give sufficient consideration to the role of user agency in promoting online safety?

The role of Ofcom

22. Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?

23. Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

24. How will Ofcom interact with the police in relation to illegal content, and do the police have the necessary resources (including knowledge and skills) for enforcement online?

If the platform providers adopt digital identity, this will enable a much-improved process for users to report misuse to the platforms, and for the platforms to report the real identity to the police and Ofcom in a timely manner. This will maximise the time that the police have to establish a case before the statutory window expires.

25. Are there systems in place to promote, transparency, accountability, and independence of the independent regulator?

26. How much influence will a) Parliament and b) The Secretary of State have on Ofcom, and is this appropriate?

27. Does the draft Bill make appropriate provisions for the relationship between Ofcom and Parliament? Is the status given to the Codes of Practice and minimum standards required under the draft Bill and are the provisions for scrutiny of these appropriate?

28. Are the media literacy duties given to Ofcom in the draft Bill sufficient?

27 September 2021